



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · POWER & ELECTRICITY

Keep the Lights On. Keep Attackers Out.

IT/OT security, ICS/SCADA assessment, SOC, remote access reviews, resilience and sector compliance for generators, transmission utilities, DISCOMs, grid operators and electricity traders.

IT/OT Security

ICS/SCADA Assessment

24/7 OT SOC

Remote Access Reviews

Resilience

CEA Compliance

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

The grid is critical infrastructure. Attackers treat it that way.

Power utilities run SCADA, substation automation and plant control systems connected to one national grid. The CEA (Cyber Security in Power Sector) Regulations, 2026—notified on 31 July 2026 and in force from 1 April 2027—now make cybersecurity a regulatory obligation.

What keeps leadership teams awake

- Nation-state intrusion into grid control systems
- Ransomware spreading from IT into OT
- Permanent vendor remote access into substations and plants
- Smart meter head-end systems with mass-disconnect power
- Legacy, unpatched control systems on flat networks
- CEA Regulations, CSIRT-Power, CERT-In and NCIIPC obligations



31 Jul 2026

CEA Cyber Security Regulations notified

1 Apr 2027

Regulations come into force

6 hours

To report incidents to CSIRT-Power and CERT-In (as reported)

50 MW

Threshold for generators and storage under the regulations

The rulebook has changed

Instrument	What it means for you
CEA (Cyber Security in Power Sector) Regulations, 2026 (31 Jul 2026)	In force 1 April 2027; senior CISO and alternate, 24-hour Information Security Division, cyber security policy, crisis management plan and annual audits (as reported)
Incident reporting	Incidents to CSIRT-Power and CERT-In within six hours (as reported); CERT-In Directions also apply
OT protection	Separation of OT networks from the internet, vendor accountability and audits of critical systems (as reported)
NCIIPC · DPDP	Protection of notified critical information infrastructure; consumer data safeguards from May 2027

One partner from plant to meter

Built around our primary proposition for the sector: **IT/OT security, ICS/SCADA assessment, SOC, remote access reviews, resilience and sector compliance.**

IT/OT Security

- IT/OT architecture and segmentation
- OT asset inventory
- IEC 62443-aligned reviews
- Removable media and endpoint controls

ICS/SCADA Assessment

- SCADA, EMS and DCS assessments
- Substation automation and relay reviews
- Safe, passive OT testing
- Smart meter head-end testing

24/7 OT SOC

- IT and OT monitoring
- Industrial protocol threat detection
- Threat hunting for state actors
- 6-hour CSIRT-Power and CERT-In reporting support

Remote Access Reviews

- Vendor and OEM access brokering
- MFA and session recording
- Jump host and DMZ reviews
- Access recertification

Resilience

- Cyber Crisis Management Plan support
- Mock drills and tabletop exercises
- OT backup and recovery testing
- Black-start and restoration planning

CEA Compliance

- CEA Regulations 2026 gap assessment
- Cyber security policy and CISO support
- Annual audits of critical systems
- Evidence and closure tracking

Who we serve: thermal, hydro and gas generators · transmission utilities · state and regional load dispatch centres · distribution companies (DISCOMs) · electricity traders and exchanges · captive and industrial power plants.

Packaged for how utilities buy

Eleven Codec Networks bundles apply directly to power utilities and grid organisations:

B1

Cyber Assessment & VAPT Assurance

B2

Application, API & DevSecOps Security

B3

Cloud, Infrastructure & Zero Trust

B4

Regulatory Cyber Audit & Compliance

B5

GRC, ISO, SOC 2 & PCI DSS Maturity

B6

Data Privacy & DPDPA Program

B7

Managed SOC, MDR & Threat Monitoring

B8

Forensics, Incident Response & Malware RCA

B9

Third-Party & Supply-Chain Risk

B10

Cyber Simulation, Awareness & Tabletop

B11

Emerging Tech, AI & Web3 Security

Foundation

Captive plants and smaller utilities

- CEA Regulations gap assessment
- IT/OT segmentation review
- Remote access review
- Cyber security policy pack

Assurance

State utilities and DISCOMs

- SCADA and substation assessments
- Smart metering security review
- Annual audit of critical systems
- 24x7 IT/OT SOC

Continuous Resilience

Large generators, transmission and grid operators

- Continuous OT testing and red teaming
- State-actor threat hunting
- Crisis management plan and mock drills
- Board and regulator reporting

Mapped to your obligations

Requirement	How we help	Bundle
Senior CISO and alternate; 24-hour Information Security Division (CEA Regulations 2026, as reported)	Governance design and CISO support	B5
Cyber security policy and Cyber Crisis Management Plan with annual mock drill (as reported)	Policy, CCMP and drill support	B5, B10
Annual audit of critical systems (as reported)	Independent IT/OT audits	B4, B1
Incidents to CSIRT-Power and CERT-In within six hours (as reported)	OT SOC, IR retainer and reporting support	B7, B8
Separation of OT networks from the internet (as reported)	IT/OT segmentation and remote access review	B3
Vendor accountability and supply-chain security	Vendor and equipment assessments	B9
Consumer and smart meter data safeguards (DPDP)	DPDPA programme for DISCOMs	B6

Why utilities choose Codec Networks

CERT-In empanelled

Independent IT/OT audits recognised by regulators.

Certified and accountable

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018 certified.

OT-safe methods

Passive discovery and planned testing that respect grid operations.

CEA-mapped

Findings mapped to the CEA Regulations 2026, CERT-In and NCIIPC expectations.

Full stack, one partner

IT/OT testing, SOC, forensics and compliance connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

Assets and sites, SCADA and plant systems, vendors and remote access, metering and your compliance calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.

START WITH A SCOPING SESSION

Let's make your next audit, drill and incident a non-event.

Tell us your assets, control systems and obligations. We will propose a practical, OT-safe assessment and assurance plan.

New Delhi

507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50, Gurugram – 122018, Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Source: CEA (Cyber Security in Power Sector) Regulations, 2026, as reported; confirm against the official gazette notification.